**PASSWORD MANAGEMENT AND CREATION POLICY**

**OVERVIEW:**

Passwords play a critical role in computer security, serving as the initial defense for user accounts. A weak password choice could potentially lead to a breach of the entire corporate network of {COMPANY-NAME}. Therefore, every individual associated with {COMPANY-NAME}, including employees, volunteers, directors, contractors, and vendors with access to {COMPANY-NAME} systems, is accountable for following the outlined guidelines to carefully choose and safeguard their passwords.

**PURPOSE:**

The Password and Management Policy serves to fortify {COMPANY-NAME}'s cybersecurity by establishing guidelines for creating strong passwords, regularly updating them, and implementing secure management practices. This policy aims to safeguard sensitive information, prevent unauthorized access, and uphold the overall integrity of {COMPANY-NAME}'s digital infrastructure.

**AUDIENCE:**

This policy is relevant to all individuals, including staff, volunteers, and directors, possessing or overseeing accounts (or any access requiring a password) on systems within {COMPANY-NAME} facilities. It extends to those with access to the {COMPANY-NAME} network or handling non-public {COMPANY-NAME} information.

**POLICY DETAIL:**

**User Network Passwords:**

Passwords for {COMPANY-NAME} network access must be implemented according to the following guidelines:

* Passwords must be changed every 90 days
* Passwords must adhere to a minimum length of 10 characters
* Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&\*\_+=?/~’;’,<>|\)
* Passwords must not be easily tied back to the account owner such as:
  + Username, social security number, nickname, relative’s names, birth date, etc.
* Passwords must not be dictionary words or acronyms
* Passwords cannot be reused for 1 year

**System-Level Passwords:**

* All system-level passwords must adhere to the following guidelines:
  + Passwords must be changed at least every 6 months
  + All administrator accounts must have 12 character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
  + Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts
  + Administrators must not circumvent the Password Policy for the sake of ease of use

**Password Protection:**

* The same password must not be used for multiple accounts.
* Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential {COMPANY-NAME} information.
* Stored passwords must be encrypted.
* Passwords must not be inserted in e-mail messages or other forms of electronic communication.
* Passwords must not be revealed on questionnaires or security forms.
* Users must not hint at the format of a password (for example, “my family name”).
* {COMPANY-NAME} passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
* Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
* If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
  + Take control of the passwords and protect them
  + Report the discovery to IT
* PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
* If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
  + Take control of the passwords and protect them
  + Report the discovery to IT
* Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with {COMPANY-NAME}.

**ENFORCEMENT:**

* Employees violating this policy may face disciplinary action, including termination, and may incur civil or criminal penalties.
* Vendors, consultants, or contractors in violation may face sanctions, including the removal of access rights, termination of contract(s), and potential civil or criminal penalties.